

**Introduction**

ServMon est un Windows dont l’adresse IP est 10.10.10.184.

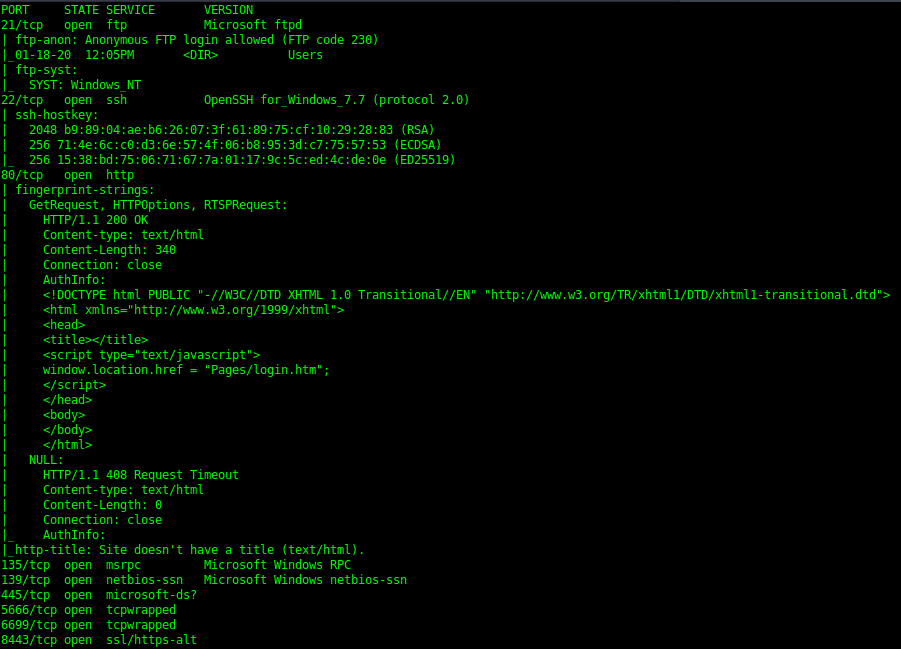
Compétences mises en œuvre :

* Enumération des ports et services.
* Vérification FTP
* Identification d’un service web vulnérable.
* Recherche et exploitation de CVE (LFI).
* CVE d’élévation de privilège sous Windows.
* Redirection de port (port forwarding sous SSH) sous Windows.
* Transfert de fichier de la machine attaquante à la victime avec scp.

**Enumération initiale**

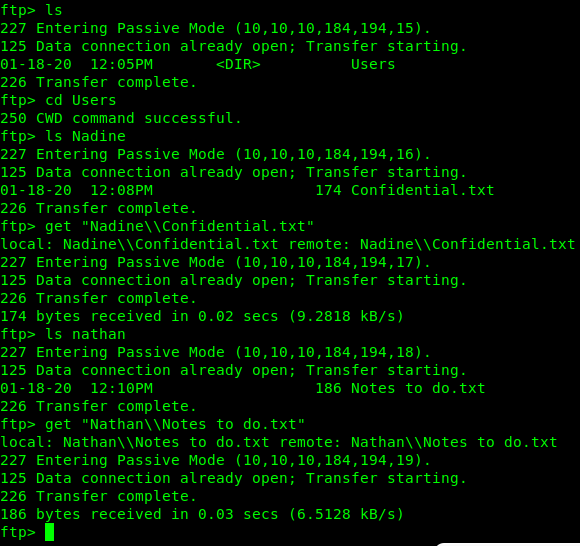
Nous commençons comme toujours par l’énumération des ports et services de la machine avec **nmap** :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.184 |



Plusieurs ports ouverts, nous allons commencer par énumérer les fichiers/dossiers accessible sur le **FTP** puis nous passerons à l’énumération des sites web.

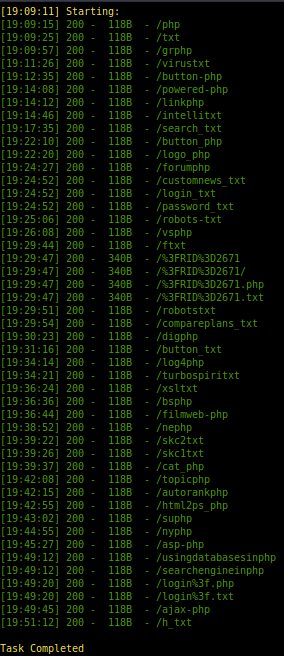
|  |
| --- |
| $ ftp  ftp > anonymous  ftp > passive  ftp > ls  ftp > cd Users  ftp > ls Nadine  ftp > get "Nadine\\Confidential.txt"  ftp > ls Nathan  ftp > get "Nathan\\Notes to do.txt" |



Les ressources obtenus lors de l’énumération ftp nous permet de savoir qu’un fichier **passwords.txt** est présent sur le bureau de l’utilisateur **Nathan**.

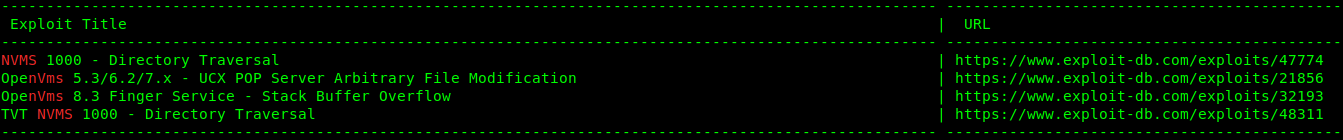
Passons maintenant les serveurs web, étant donné qu’il y en a deux, nous allons nous attarder sur le normal (**port 80**) avec une énumération de dossier/fichier avec **dirsearch** :

|  |
| --- |
| $ dirsearch –w wordlist.txt –e "php,txt" –f –x 403 –t 80 –u http://10.10.10.184 |



En attendant la fin d’énumération, nous allons effectuer un rapide tour sur l’interface web, nous pouvons voir que la technologie utilisée est : **NVMS-100** . Nous allons donc rechercher une CVE ou un exploit concernant **NVMS** avec **searchsploit** et google :

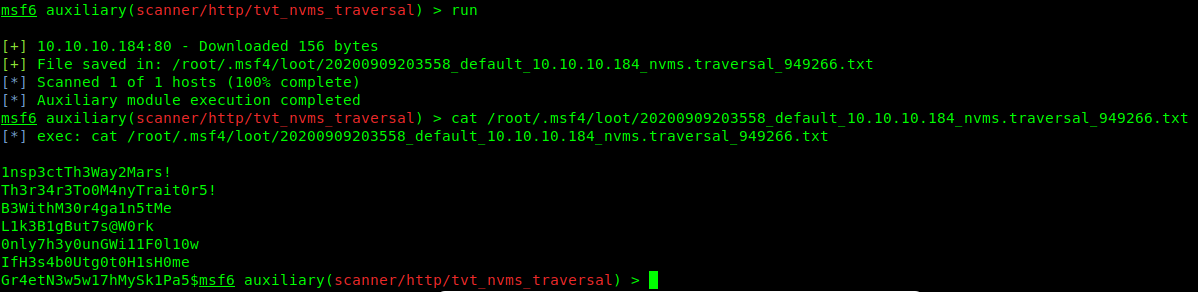
|  |
| --- |
| $ searchsploit NVMS |



**Obtenir un accès utilisateur**

Le deuxième exploit est testé et approuvé via **metasploit**, grâce à lui, nous pouvons aller consulter le fichier sur le bureau de **Nathan** pour avoir des mots de passes :

|  |
| --- |
| $ msfconsole  Msf > use auxiliary/scanner/http/tvt\_nvms\_traversal  Msf > set rhosts 10.10.10.184  Msf > set filepath /users/nathan/desktop/passwords.txt  Msf > run |



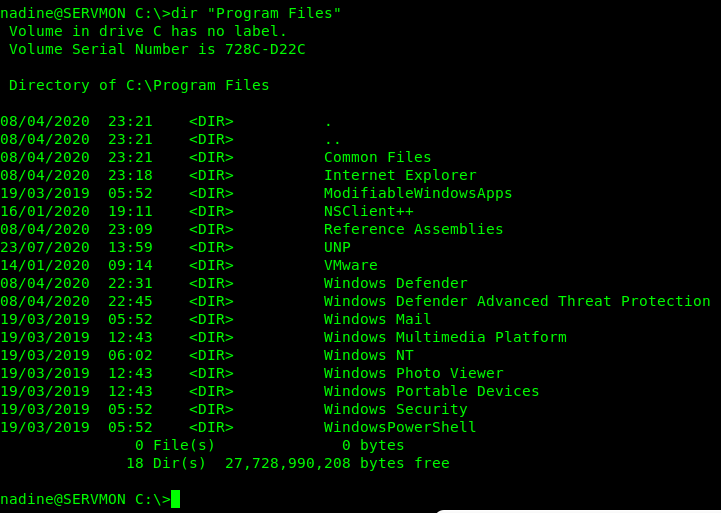
Maintenant que nous avons une liste de mot de passe, nous pouvons les tester un par un avec les identifiants **nathan** et **nadine**. Le mot de passe **L1k3B1gBut7s@W0rk** fonctionne avec **nadine**, nous pouvons aller récupérer le flag user :



**Obtenir un accès root**

L’accès root est plutôt complexe, il faut commencer avec de l’énumération des programmes installés :

|  |
| --- |
| C:\> dir "Program Files" |



Le logiciel **NSClient++** n’est pas installé par défaut par Windows, il est donc très suspect. Un tour sur **exploit-db** permet de trouver un exploit :

<https://www.exploit-db.com/exploits/46802>

Toutes les étapes sont détaillées dans l’exploit et comment les effectuer, en résumé :

* Obtenir le mot de passe de l’administrateur de l’interface web.
  + **C:\> type "C:\Program Files\NSClient++\nsclient.ini"**
* Activer des modules permettant l’appel de script.
* Transférer netcat et un script bat à la victime.
* Mettre un listener netcat en écoute.
* Ajouter le script bat sur l’interface web victime.
* Planifier une tache pour déclencher le script.
* Attendre pour avoir la session et récupérer le flag root.

Pour se connecter sur l’interface web, comme le service tourne en local, il faut faire une redirection de port en ssh sur la machine attaquant :

|  |
| --- |
| $ ssh –L 8443 :127.0.0.1 :8443 nadine@10.10.10.184 |

(Tout le traffic entrant en 8443 est redirigé sur 127.0.0.1 sur le port local 8443)

[root]